AUSA: Ryan B. Finkel

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

KAI WEST,
a/k/a "IntelBroker,"
a/k/a "Kyle Northern,"

Defendant.

25 MAG 567

SEALED COMPLAINT

Violations of 18 U.S.C. §§ 371, 1030, 1343, 1349, and 2

COUNTY OF OFFENSE:
NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

CARSON HUGHES, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), and charges as follows:

COUNT ONE
(Conspiracy to Commit Computer Intrusions)

1. From at least in or about December 2022 through at least in or about February 2025, in the Southern District of New York and elsewhere outside of the jurisdiction of any particular State or district of the United States, KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit offenses against the United States, to wit, a computer intrusion and intentionally causing damage to a computer system, in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(c)(3)(A), 1030(a)(5)(A), 1030(c)(4)(A)(i)(I)(II)(VI), and 1030(c)(4)(B)(i) and (ii).

2. It was a part and an object of the conspiracy that KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, and others known and unknown, knowingly and with the intent to defraud, would and did access a protected computer without authorization, and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value, in violation of Title 18, United States Code, Sections 1030(a)(4) and (c)(3)(A).

3. It was further a part and an object of the conspiracy that KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, and others known and unknown, knowingly would and did cause the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage, without authorization, to a protected computer, which caused a loss (including loss resulting from a related course of conduct affecting one and more other protected computers) aggregating to at least $5,000 in value to one and more persons during any one-year period, and which caused the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals, and which affecting 10 or more protected computers during any 1-year

period in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I)(II)(VI) and 1030(c)(4)(B)(i) and (ii).

Overt Acts

a. On or about January 6, 2023, WEST and his co-conspirators exfiltrated data from a victim, and deleted files controlled by that victim, which caused at least $5,000 in damages.

b. On or about January 6, 2023, in the Southern District of New York and elsewhere, WEST, using the IntelBroker username, offered for sale data stolen from a victim.

c. On or about March 6, 2023, WEST and his co-conspirators exfiltrated patient data, including health care information, from a medical services provider and in so doing caused the modification or impairment, or potential modification or impairment, of patient medical care.

(Title 18, United States Code, Sections 371 and 3238.)

COUNT TWO
(Conspiracy to Commit Wire Fraud)

4. From at least in or about December 2022 through at least in or about February 2025, in the Southern District of New York and elsewhere outside of the jurisdiction of any particular State or district of the United States, KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

5. It was a part and object of the conspiracy that KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, and others known and unknown, knowingly having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, WEST and others engaged in a scheme to use fraudulent means to access without authorization computer networks of victims, exfiltrate data from those networks, and sell that data for profit, which involved the use of interstate and foreign wires into and out of the Southern District of New York.

(Title 18, United States Code, Section 1349 and 3238.)

COUNT THREE
(Accessing a Protected Computer to Defraud and Obtain Value)

6. From at least in or about December 2022 through at least in or about June 2023, in the Southern District of New York and elsewhere outside of the jurisdiction of any particular State or district of the United States KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the

defendant, who is expected to be first brought to and arrested in the Southern District of New York, knowingly and with the intent to defraud, would and did access a protected computer without authorization, and exceed authorized access, and by means of such conduct further the intended fraud and obtain anything of value, to wit, WEST entered, and aided and abetted, the hack of a victim's system without authorization, exfiltrated data from that victim, and sold that data, using the IntelBroker username, on an online forum.

(Title 18, United States Code, Sections 1030(a)(4), (c)(3)(A), 3238 and 2.)

COUNT FOUR
(Wire Fraud)

7. From at least in or about December 2022 through at least in or about February 2025, in the Southern District of New York and elsewhere outside of the jurisdiction of any particular State or district of the United States, KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, who is expected to be first brought to and arrested in the Southern District of New York, the defendant, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, to wit, WEST and others engaged in a scheme to use fraudulent means to access without authorization computer networks of victims, exfiltrate data from those networks, and sell that data for profit, which involved the use of interstate and foreign wires into and out of the Southern District of New York.

(Title 18, United States Code, Sections 1343, 3238, and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

8. I am a Special Agent with the FBI, currently assigned to a cyber intrusion squad. This Affidavit is based upon my personal participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals. Because this Affidavit is being submitted for the limited purpose of demonstrating probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

Overview

9. For reasons explained herein, I know that "IntelBroker" is the online moniker of KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, who, in concert with his co-conspirators, compromises victims' (typically companies) computer systems, exfiltrates data from those systems (e.g. customer lists and company marketing data), and then sells the stolen data for profit. WEST accomplishes his scheme in connection with his leadership of an online hacking group which is presently called the "CyberN[------]." WEST, using the IntelBroker identity, and the online hacking group "CyberN[-----] further their illegal scheme primarily through a particular internet forum ("Forum-1").

10. As set forth below, KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, and his co-conspirators participated in computer intrusions and thefts of data from multiple U.S. victim companies between approximately 2023 to 2025, and publicly tried to sell, or otherwise distribute, the property they stole on Forum-1. Based on my review of WEST's public messages (using the IntelBroker moniker), from in or about January 2023 through in or about February 2025, WEST has offered hacked data for sale approximately 41 times; and offered to distribute hacked data for free (or for Forum-1 credits, which are explained *infra*) approximately 117 times. WEST, and his co-conspirators, have sought to collect at least approximately $2,000,000 by selling the stolen data. Based on FBI communications with the victims of these breaches, WEST and his co-conspirators have cumulatively caused victim losses of at least approximately $25,000,000.

11. Based on my review of publicly available information, including accessing Forum-1 and its contents, I know that:

a. KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, , using the IntelBroker identity, and the online hacking group "CyberN[-----] further their illegal scheme primarily through Forum-1. Forum-1 can be accessed from any internet connection, and I have accessed the site on many occasions and am familiar with it. Forum-1 is an online discussion community that is focused on computer network intrusions, which is commonly known as "hacking." When joining Forum-1 a user creates a "username," which is the name by which the user is known on Forum-1. (WEST selected the username "IntelBroker.") Each user on Forum-1 can associate their username with an image and, if they so choose, a signature block. The image and signature block serve to identify a user on Forum-1 and can help the user gain notoriety within the Forum-1 community. When logged into Forum-1 each user can post public messages under their username, users can publicly respond to public messages made by others (creating a conversation "thread"), and users can communicate privately via a private message service. Unless deleted, public messages, and conversation threads, persist on Forum-1.[1] Forum-1 also offers users "credits" for participating on the site. As a user obtains more credits, their "level" on the site increases thereby providing them notoriety and access to additional features. Credits can be traded on the site between users.

b. I have reviewed content that WEST, using the IntelBroker username, posted on Forum-1 while accessing the site from, among other places, Manhattan, New York. Based on my review, WEST (using the IntelBroker moniker) is a prolific user of Forum-1. As of in or about February 2025, IntelBroker's profile on Forum-1 indicates WEST has posted approximately 335 public messages (*i.e.* the first post which started a conversation thread). WEST also posted approximately 2,126 individual comments or responses within conversation threads. While the

[1] Forum-1 was originally launched in or about March 2022 until it was shutdown by law enforcement in or about March 2023. The second iteration of Forum-1 launched in or about June 2023 but was temporarily taken offline on or about May 15, 2024. Forum-1 relaunched on or about May 29, 2024 and remains active. Public messages, comments, threads, and private messages from the first version of Forum-1 are no longer available on the site, however, information from in or about June 2023 through the present remains available on Forum-1. For simplicity, I refer to all the iterations collectively as "Forum-1" unless otherwise noted.

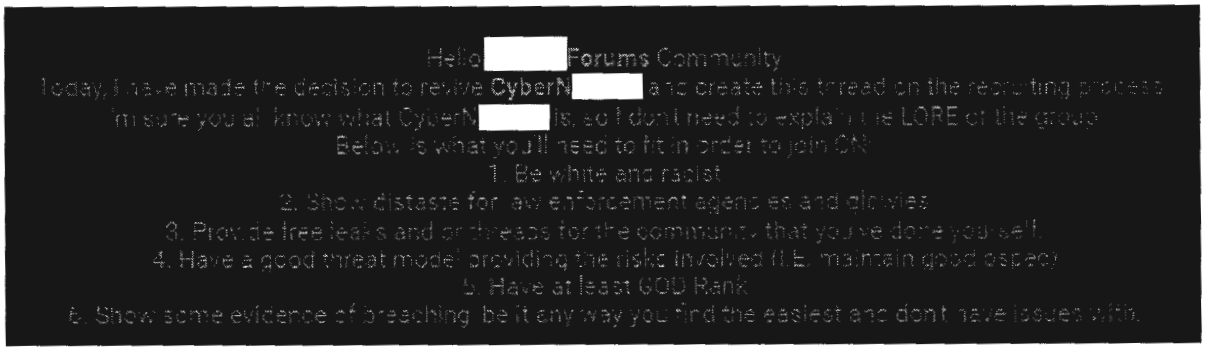
topics of those threads vary, as explained herein, a significant percentage of the threads started by WEST offer compromised victim data for sale. WEST (using the IntelBroker moniker) has sold stolen data on Forum-1 since at least in or about January 2023 and continues to do so through in or about February 2025. Based on a review of WEST's IntelBroker posts, and by way of example, I have viewed approximately 158 threads started by WEST that offer stolen data for sale, for Forum-1 credit, or for free, since in or about January 2023 through in or about February 2025. At least approximately 41 of those 158 public messages sell data from companies based in the United States. Of those 158 messages, approximately 16 provided a specific asking price for the stolen data, which cumulatively totals at least approximately $2,467,000. At least approximately 25 of the 158 public messages invited Forum-1 users to private message IntelBroker (*i.e.* WEST) to negotiate a sales price. The remaining 117 public messages offer hacked data for free to Forum-1 users or in exchange for Forum-1 credits.[2] At least approximately 46 of the 158 public messages indicate that WEST worked in concert with a particular Forum-1 user ("CC-1") to obtain the data through a "breach" (*i.e.* "hack"). WEST's public messages (as IntelBroker) indicate that he accepts payment via Monero, which is a cryptocurrency[3] that uses a blockchain with privacy-enhancing technologies to attempt to obfuscate transactions and seek to achieve anonymity and fungibility.

c. WEST's prolific posting (as IntelBroker), and his sales of stolen data, have generated notoriety for the IntelBroker identity within the Forum-1 community. Indeed, from in or about August 2024 through in or about January 2025, "IntelBroker" was identified on Forum-1 as the site's "owner." To further his username's notoriety, WEST has associated different images with IntelBroker but primarily uses the following image as his calling card:

[2] Based on my training and experience, a user of Forum-1 may offer stolen data for free in order to increase their notoriety on Forum-1, attract a following of Forum-1 users, establish credibility, and, in turn, be able to charge higher prices for stolen data in the future.

[3] Cryptocurrency is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it. Asset records are maintained by a digital ledger (also known as a blockchain), which is a computerized database that tracks cryptocurrency ownership. The digital ledger is maintained by a decentralized network of computing devices throughout the world. Cryptocurrencies are highly volatile and can be purchased through a number of methods, including through cryptocurrency exchanges, which are online services that enable users to exchange fiat currency (*e.g.* U.S. Dollars) for cryptocurrencies.

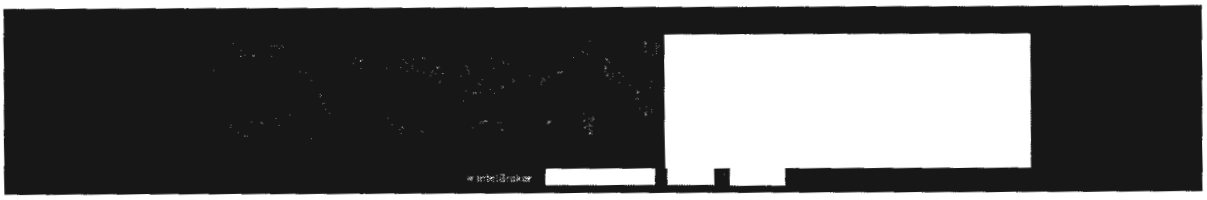
d. WEST's Forum-1 public messages (using the IntelBroker moniker) state that he works with other Forum-1 users in a collective to obtain, and distribute, victim data. As mentioned, WEST's group is presently known as the "CyberN[------]." On or about August 5, 2024, WEST authored a Forum-1 public message, with the IntelBroker username, which I have reviewed, that sought to recruit Forum-1 members to join his hacking group. This recruitment message is reproduced, in part, below:



This August 5, 2024, recruitment message also appears to be a mission statement of the CyberN[------]. Based on my review of WEST's IntelBroker public messages, the group's members have varied overtime. In addition, in or about early 2023 the group was known as "The boys" before it adopted its current name. Despite those changes, based on my review of Forum-1 public messages, it appears that at all times the group was focused on illegally acquiring victim data via illegal intrusions of computer networks and selling, or distributing, it to Forum-1 users.

e. To reflect his membership in this online group presently known as the CyberN[------]," WEST, using the IntelBroker username, created a signature block on Forum-1 that lists other members of the group, and the group's name, at a particular time. For example, when the group was known as "The boys" IntelBroker signed his public messages with, among other things, the following:

Following that text were a list of usernames who belonged to the group. More recently, including in or about February 2025, WEST has used a signature block for IntelBroker similar to the following:



f. On Forum-1 when a user updates their signature block, or their associated icon, the new signature block and icon apply to all of that user's public posted messages moving forward as well as all that user's previous messages. Accordingly, as of in or about February 2025, all of IntelBroker's Forum-1 public messages since in or about June 2023 (when the second iteration of Forum-1 launched) are associated with the CyberN[------] including all messages in which IntelBroker offered for sale compromised victim data. Based on my training and experience, and my review of Forum-1, I believe that WEST's decision to associate all of his "hacking" activity with his online hacking group increased the notoriety of the CyberN[------], which, in turn, increases the group's ability to recruit members, acquire victim data, sell victim data, and further the goals of the conspiracy.

Examples of WEST's Hacking Activity Using the IntelBroker Moniker

January 2023 - WEST Illegally Obtains Victim-1 Stolen Data and Sells it Online

12. Based on my review of Forum-1 posts and other publicly available information, conversations with victim witnesses described below, and conversations with other law enforcement personnel regarding the same, I have learned the following, among other things:

a. On or about January 6, 2023, KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, using the IntelBroker moniker authored a public message on Forum-1 titled "[Victim-1] Ransomware Leak." In that message, which is reproduced in part below, WEST (as IntelBroker) boasted that he had acquired Victim-1's data, which WEST offered for a "five-digit sum of XMR [*i.e.* Monero]."[4] Victim-1 is a U.S.-based telecommunications provider. Apparently to prove that IntelBroker had, in fact, stolen Victim-1's data the January 6 message allowed Forum-1 users to access a "sample" of the data.

b. The January 6 message also referenced approximately 32 members of "The Boys," approximately 28 of which were referenced in a subsequent IntelBroker message as members of the CyberN[------] including, for example, a March 6, 2023 message, which is further described *infra* ¶ 13.a.

c. Victim-1's digital forensics personnel informed the FBI that they had reviewed IntelBroker's January 6 public message, analyzed the "sample" data, and determined it was authentic Victim-1 data. Specifically, the data contained information related to Victim-1's marketing toward its customers. Victim-1 further determined that the data was stolen from another particular company ("Victim-2"), which Victim-1 had contracted with to store data and perform other services. Through communications with Victim-2, Victim-1 determined that an

[4] On or about January 6, 2023, 10,000 Monero was equivalent to approximately $1,550,000.

unauthorized actor who, for reasons explained herein I believe is WEST, accessed Victim-2's systems without permission and exfiltrated data. Based on communications with Victim-2, Victim-1 determined that the unauthorized access originated from two particular IP addresses (the "Attack IPs").

d. Victim-2 is an internet service provider that assists businesses in harnessing the internet for commerce and advertising. In carrying out these functions, Victim-2 sometimes stores data for its clients on servers Victim-2 controls. Victim-2 is based in Manhattan, New York. Based on statements made by Victim-2's representatives to the FBI, I have learned that, on or about January 6, 2023, Victim-1 contacted Victim-2 to alert it that Victim-1 data, which Victim-2 stored had been leaked online. Victim-2 subsequently performed an investigation and determined that an unauthorized actor—who for reasons explained herein I believe is WEST—was able to infiltrate a server Victim-2 controlled. That server used a particular software ("Software-1"), which had been improperly configured such than an unauthorized individual could access the server without any login credentials. Victim-2 assessed that the unauthorized access occurred from at least on or about December 29, 2022 through on or about January 6, 2023. Victim-2 advised the FBI that the actor—who I believe is WEST—downloaded approximately 3,569 objects (*i.e.* documents and files) and deleted approximately 45 objects after gaining access to Victim-2's server. To identify, and remedy, the aforementioned breach, Victim-2 spent several hundred thousand dollars.

March 2023 - WEST Illegally Obtains Victim-3 Stolen Data and Sells it Online

13. Based my review of Forum-1 posts and other publicly available information, conversations with victim witnesses described below, and conversations with other law enforcement personnel, including an undercover law enforcement officer ("UC-1"):

a. On or about March 6, 2023, KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, using the IntelBroker moniker authored a public message on Forum-1 titled "CyberN[------] [redacted reference to Victim-3] Database." In that message, WEST (as IntelBroker) wrote, in part, "[i]n the last hour, CyberN[------] members breached [Victim-3]. I am in possession of the data and I am now selling it here. . . . I am looking for an undisclosed amount in XMR crypto currency." On or about March 6, 2023, the message's signature block contained the logo of the CyberN[------] and listed its then-approximately 40 members—approximately 28 of which previously listed as members of "the Boys" in the January 6, 2023 message described above, *supra* ¶ 12.b.

b. Beginning on or about March 6, 2023, through at least on or about March 14, 2023, Victim-3, which is a municipal Government healthcare provider, issued a series of public statements confirming, in substance and in part, that an unauthorized person or persons obtained patient data from their systems including name, Social Security number, date of birth, gender, health plan information (*e.g.*, plan name, carrier name, premium amounts, employer contribution, and coverage dates), employer information, enrollee information (e.g., address, email, phone number, race, ethnicity, and citizenship status). Victim-3 further stated, in substance and in part, that it hired an independent investigative firm to ensure the compromise was halted and were paying for any impacted client's credit monitoring for three years.

c. On or about March 7, 2023, UC-1 contacted "IntelBroker" via Forum-1 and purchased the Victim-3 data for approximately $1,000 in Monero. Thereafter, IntelBroker

provided the undercover law enforcement officer a download link, which appeared to contain data from Victim-3—*i.e.* data of approximately 56,415 individuals including health insurance data for those individuals.

August 2024 - WEST Illegally Obtains Victim-4 Stolen Data and Sells it Online

d. On or about August 25, 2024, KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, using the IntelBroker moniker, authored a public message on Forum-1 titled "[Victim-4] Internal Communications." In that message WEST (as IntelBroker) wrote that "[t]oday, I'm selling the [Victim-4] internal communication breach. This breach was conducted today." IntelBroker did not specify a price for the data from Victim-4. Apparently to prove that WEST had, in fact, stolen Victim-4's data, the August 25 message provided Forum-1 users a "sample" of the data. As of in or about February 2025, this message contained IntelBroker's signature block which references the CyberN[------] and its now present membership of four individuals including CC-1.

e. Employees of Victim-4 informed the FBI, in substance and in part, that they had reviewed the sample data in the August 25 IntelBroker public message and determined that it was authentic Victim-4 data, which had been stored by another company ("Victim-5"). Based on information from Victim-5, and the nature of the information in the sample, Victim-4 assessed that the data was obtained by unauthorized access to, or by exploiting a vulnerability in, an API.[5] Because Victim-4 did not house the stolen data, – Victim-4's representatives were unable to provide detail on how the data had been obtained.

November 2024 - WEST Illegally Obtains Victim-6 Stolen Data and Sells it Online

f. On or about November 22, 2024, KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, using the IntelBroker username authored a public message on Forum-1 titled "[Victim-6] ISP." In that message WEST wrote that "Today, I'm selling the entire database to [Victim-6], an ISP based in the USA and provides internet access ot a range of countries. . . . below is the sample . . . . If you wish to buy this data please message me . . . XMR ONLY." The public message further stated, "Breached by: @IntelBroker & [CC-1]." As of in or about February 2025, this message contained IntelBroker's signature block which references the CyberN[------] and its present membership of four individuals including CC-1.

g. Employees of Victim-6 informed the FBI, in substance and in part, that they had reviewed the sample data in the November 22 IntelBroker public message and determined that it was authentic Victim-6 data. Victim-6 employees further assessed that the intruder used information from another unauthorized leak of Victim-6 data to compromise one of their servers.

KAI WEST is "IntelBroker"

14. Based on my review of documents, including judicially authorized search warrant returns and the publicly available Bitcoin blockchain, conversations with an undercover law

[5] An API or an "application programming interface," is software which enables communications between two different computer programs.

enforcement officer ("UC-2"), conversations with witnesses, law enforcement personnel and others, I have assessed that KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, is "IntelBroker" based on the following, among other things:

Undercover Purchase from "IntelBroker" Leads to WEST's Cryptocurrency Accounts

a. On or about January 26, 2023, WEST (using the IntelBroker moniker) offered for sale on Forum-1 an API Key for a particular victim ("Victim-7") for $250 in Monero.[6] This Forum-1 public message did not reference working with other Forum-1 users.

b. On or about January 26, 2023, UC-2 sent a private message to "IntelBroker" (*i.e.* WEST) via Forum-1 requesting to purchase the Victim-7 data. Over several messages, UC-2 asked IntelBroker (*i.e.* WEST) to sell the Victim-7 data for $250 in Bitcoin, which is a cryptocurrency that does not have the same privacy-enhancing technologies as Monero. WEST (using the IntelBroker moniker) provided UC-2 a particular Bitcoin wallet address ("BTC Wallet-1"),[7] and after UC-2 sent payment to IntelBroker, IntelBroker provided UC-2 the Victim-7 API Key as well as three purported administrator logins with a password for those logins.[8]

c. FBI personnel analyzed BTC Wallet-1's transactions on the Bitcoin blockchain and learned, *inter alia*: Prior to on or about January 26, 2023, BTC Wallet-1 engaged in approximately four transactions. The first transaction occurred on or about October 12, 2022 when BTC Wallet-1 received .00036551 Bitcoin from a particular wallet ("West Wallet-1"). That is, West Wallet-1 appears to have seeded (i.e. provided an initial set of funds to) BTC Wallet-1. Based on my training and experience, this indicates that the owner of West Wallet-1 and BTC Wallet-1 are at least associated with each other.

d. The same day—on or about October 12, 2022—West Wallet-1 was created by a Ramp account ("Ramp Account-1").[9] Based on my training and experience, this further suggests that the owner of West Wallet-1 and Ramp Account-1 are associated with each other. Also, that

---

[6] An API Key is a unique string of characters that acts as a secret identifier, used to authenticate and authorize an application or user when accessing an API.

[7] A Bitcoin wallet stores a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet.

[8] Based on communications with the FBI, personnel responsible for storing the Victim-7 API Key, analyzed the API Key IntelBroker sold to UC-2. That personnel determined that API Key was the same API key used to extract publicly available data from Victim-7's website and is an API Key that anyone can obtain after registering with Victim-7. With respect to the administrator usernames, the personnel advised that they appear to be legitimate administrator usernames. With respect to the password, that password is the default password which Software-1 (*i.e.* the same software exploited in the Victim-1 and Victim-2 hack) sets when a user resets their password.

[9] Ramp is an online bank and financial management provider.

same day—on or about October 12, 2022—Ramp Account-1 was created. This further demonstrates a link between BTC Wallet-1, West Wallet-1 and Ramp Account-1 because it indicates that West Wallet-1 and Ramp Wallet-1 were created for a particular purpose—apparently the seeding of BTC Wallet-1. Indeed, based on my training and experience, this financial structuring suggests that BTC Wallet-1 was created as a "pass through" wallet—*i.e.* a wallet to obscure the funds from Ramp Account-1. That is, the owner of Ramp Account-1 created West Wallet-1, and then seeded BTC Wallet-1, to create transactions separating Ramp Account-1 from BTC Wallet-1's cryptocurrency transactions. This is a common technique used by malicious cyber actors to try to obscure their true identity.[10]

e. Ramp Account-1 is associated with a particular United Kingdom Provisional Driving License with the name "Kai Logan West" ("West License-1") with a particular date of birth ("West DOB-1").[11] That is, Ramp-1 Account was registered by KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant.

f. West License-1 is also associated with a particular Coinbase account created on or about May 5, 2020 ("West Coinbase Account-1").[12] West Coinbase Account-1 is registered in the name of "Kyle Northern," however, based on "Know-Your-Customer" (KYC) data the identity associated with West Coinbase Account-1 is "Kai West," with a date of birth that is West DOB-1, and an address in the United Kingdom. Accordingly, West Coinbase Account-1 appears to be owned and controlled by KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, and "Kyle Northern" appears to be another alias used by WEST.

West Email Account-1 is KAI WEST's Personal Email Account

g. Ramp Account-1 and West Coinbase Account-1 are registered to a particular email account ("West Email Account-1"). Based on my training and experience, I know that users typically choose to give to providers an email address over which they have domain and control, and I have found this to be true in the specific context of cybercriminals' use of various email accounts and accounts maintained by cryptocurrency exchanges.

h. Based on my review of the content of West Email Account-1, which I have accessed pursuant to a judicially authorized search warrant, West Email Account-1 appears to be a personal email account used by WEST. I believe this because, among other things:

---

[10] The same day—on or about October 12, 2022—BTC Wallet-1 sent its entire balance of .00036551 Bitcoin to a wallet associated with a virtual currency exchange (and that transaction appears to be associated with an account for an individual based in another European country ("Individual-1")). I have taken investigative steps to assess whether Individual-1 controlled BTC Wallet-1 and could be Intelbroker. However, for the reasons set forth herein, I believe the evidence demonstrates that "Kai West" owns and controls BTC Wallet-1, and is IntelBroker. Rather, as indicated herein, I believe the evidence demonstrates that "Kai West" owns and controls BTC Wallet-1, and is IntelBroker.

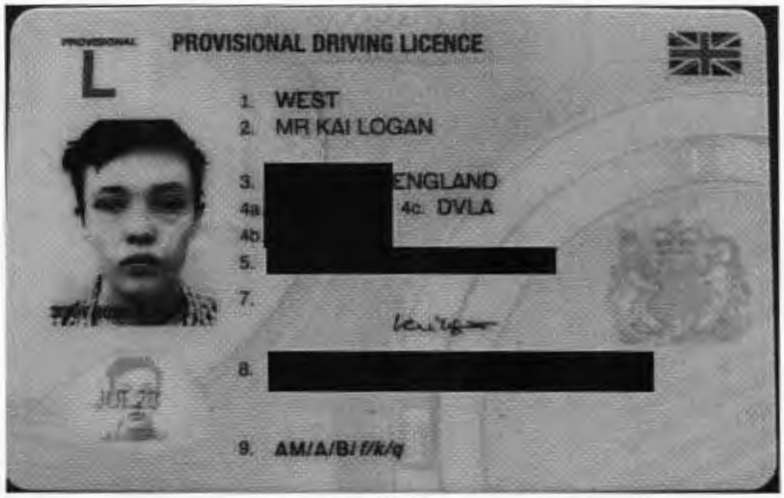
[11] "Logan" is WEST's middle name.

[12] Coinbase is an online virtual currency trading platform.

i. On or about September 22, 2022, West Email Account-1 received an invoice for data storage which was addressed to "Kai West" with an address in the United Kingdom.

ii. From on or about November 22, 2022 through on or about June 19, 2024, Email Account-1 received approximately nine emails from an email account associated with a particular United Kingdom university's housing program. Approximately six of those emails were addressed to "Kai" or "Kai Logan." The same university's finance department sent West Email Account-1 approximately four emails from on or about January 12, 2023 through on or about May 2, 2023 and all of those emails were addressed to "Kai."

iii. On or about November 29, 2022, West Email Account-1 received an email from an email account with the username "Kyle.Northern1337" with a photograph of West License-1.[13] As indicated above "Kyle Northern" is an alias used by WEST. Based on my training and experience, I have learned that "1337" is slang used in online hacker communities which stands for "Leet" (what 1337 appears to be when held upside down) and is short for "elite." The photograph of West License-1 is reproduced, with redactions, below:



iv. On or about September 28, 2023, West Email Account-1 sent an email that attached a "Certificate of Student Status Academic Year 23/24" for "Kai West" with West DOB-1.

[13] Based on my review of the contents of the Kyle.Northern1337 email account, also obtained pursuant to a judicially authorized search warrant, I know that the Kyle.Northern1337 email account is subscribed in the name of "Kai West." The Kyle.Northern1337 email account contains the following images stored in a cloud-based server associated with that account: (i) several selfies of the same individual who appears in West License-1; (ii) a screenshot with "Payment Info," including the name "Kai West"; (iii) a screenshot of an article titled "FBI seizes [redacted], a website that sold access to breached data"; (iv) images of receipts with the name "Kai West"; and (v) videos of a command-line tool called "GPRS Smash," which is networking software that would be of interest to cybercriminal such as IntelBroker.

That certificate further stated, in part: "Programme of Study BA/BSc/LLB/MSc with Foundation Year - Cyber Security."

v. On or about November 9, 2023, West Email Account-1 received an email from a particular email address ("West Email Account-2"),[14] which email contained a photograph of West License-1.

vi. On or about April 30, 2024, West Email Account-1 forwarded the November 9, 2023 email referenced immediately above back to West Email Account-2.

Accounts Registered to West Email Account-1 Used the Same IP Addresses as "IntelBroker" During the Same Time Frames

i. Based on my review of documents from Microsoft pursuant to a § 2703(d) order, a Microsoft account registered to West Email Account-1 was accessed from the Attack IPs between on or about January 6, 2023, and on or about January 8, 2023, a timeframe during which Victim-2's servers were compromised by IntelBroker and Victim-1's data was extracted, *see supra* ¶ 12.c.

j. A particular X (formerly known as Twitter) account in the name of "IntelBroker," which was registered to email address intelbroker@[redacted].shitposting.[redacted], was created on or about December 4, 2023 from a particular IP address, which is an IP address registered to a particular VPN.[15] Between on or about September 6, 2023, and on or about March 23, 2024, West Email Account-1 was accessed by that same IP address approximately 22 times.

WEST's Online Activities Correlate to "IntelBroker's" Activities

k. Based on my review of records obtained pursuant to judicially-authorized search warrants for the WEST email accounts described above, I have learned that WEST, while using West Email Account-1, viewed several YouTube videos shortly before the IntelBroker username posted public messages about those same videos on Forum-1. For example:

i. On or about July 11, 2023, beginning at 12:06 UTC through 12:08 UTC, West Email Account-1 viewed a video on YouTube titled "kobo requested the ara ara ctto:@nvcnouu." The same day at approximately 12:09 UTC, based on a publicly available

---

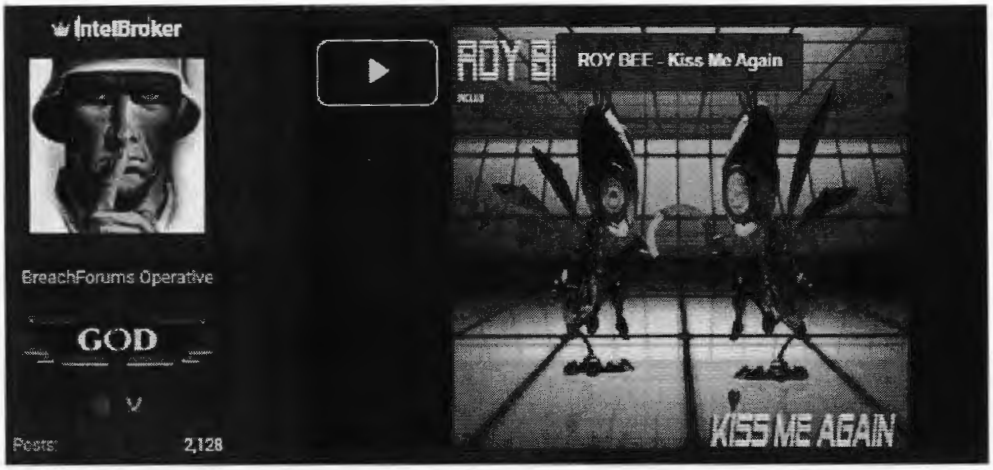
[14] West Email Account-2 also appears to be a personal email account used by WEST. Based on my review of records obtained from a judicially authorized search warrant, West Email Account-2 included several emails addressed to "Kai" or "Kai West." For example, on or about September 17, 2022 Apple sent an invoice to West Email Account-2 that was addressed to "Kai West." On or about August 31, 2022, West Email Account-2 received an email from Criminal Records Office in the United Kingdom addressed to "Kai West."

[15] A VPN, or virtual private network, is a network which establishes a digital connection between a computing device and a remote server owned by a VPN provider. Accessing the internet in this fashion obscures one's true IP address. While VPN's have legitimate uses, they are also used by cybercriminals to attempt to obfuscate their identity.

Forum-1 message which I have reviewed, "IntelBroker" posted that same particular YouTube video to Forum-1.

ii. On or about January 28, 2024, through on or about February 5, 2024, West Email Account-1 viewed a video on YouTube titled "CHCL SOUP – DARKSIDE" approximately 12 times including on or about February 5, 2024 at approximately 13:14 UTC. That same day at approximately 13:15 UTC, based on a publicly available Forum-1 message which I have reviewed, "IntelBroker" posted that same particular YouTube video to Forum-1.

iii. Beginning on or about April 5, 2024 at 23:38:50 UTC, to on or about April 6, 2024 at 05:17, West Email Account-1 watched a particular YouTube music video titled "ROY BEE – Kiss Me Again," an electronic-style song, approximately three times. On or about April 6, 2024, at 05:18 UTC, based on a publicly available Forum-1 message which I have reviewed, "IntelBroker" posted that same YouTube video to Forum-1, as pictured below:



l. Based on my review of search warrant returns, I have learned that WEST, while using West Email Account-1, viewed several YouTube videos regarding IntelBroker and IntelBroker's victims. For example:

i. On or about April 2, 2024, West Email Account-1 viewed a YouTube video titled "[Victim-9] Just Had a HUGE Data Leak! Here's EVERYTHING You Should Know." Approximately two days prior, on or about March 31, 2024, WEST (using the IntelBroker moniker) authored a public message on Forum-1 in which WEST stated, in part, "Hello [Forum-1] Community, Today I have uploaded the [Victim-9] Database for you to download, thanks for reading and enjoy!"

ii. Approximately four times, on or about January 6, 2024, West Email Account-1 viewed a YouTube video titled "9; IntelBroker." I have watched this video, which is a an approximately 16-minute video featuring an interview of someone who purports to be IntelBroker. The video is in German, and I used YouTube automated features to translate it into English. During the interview the person purporting to be "IntelBroker" discusses their hacking exploits. The interviewer assesses, in substance and in part, that he believes the individual he

interviewed, purporting to be IntelBroker, speaks Serbian and Russian, and does not speak English very well. For the reasons described herein, I believe that WEST, who is IntelBroker, is from the United Kingdom, and based on his email accounts speaks fluent English.

iii. Approximately three times between January 2024 and May 2024, West Email Account-1 viewed a YouTube video titled "IntelBroker." I have watched this video, which is an approximately 1 minute and 46 second video containing news clips about the Victim-3 hack set to electronic music.

WHEREFORE, I respectfully request that a warrant be issued for the arrest of KAI WEST, a/k/a "IntelBroker," a/k/a "Kyle Northern," the defendant, and that he be arrested, and imprisoned or bailed, as the case may be.

/s authorized electronic signature

Carson Hughes
Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission of
this Complaint by reliable electronic
means (telephone), this 18th day of February, 2025.

THE HONORABLE SARAH NETBURN
Chief United States Magistrate Judge
Southern District of New York